[H.A.S.C. No. 114–117]

HEARING

ON

NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2017

AND

OVERSIGHT OF PREVIOUSLY AUTHORIZED PROGRAMS

BEFORE THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES
ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES HEARING

ON

FISCAL YEAR 2017 INFORMATION TECHNOLOGY AND CYBER PROGRAMS: FOUNDATIONS FOR A SECURE WARFIGHTING NETWORK

HEARING HELD
MARCH 22, 2016

U.S. GOVERNMENT PUBLISHING OFFICE
20–077 WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

JOE WILSON, South Carolina, *Chairman*

JOHN KLINE, Minnesota
BILL SHUSTER, Pennsylvania
DUNCAN HUNTER, California
RICHARD B. NUGENT, Florida
RYAN K. ZINKE, Montana
TRENT FRANKS, Arizona, *Vice Chair*
DOUG LAMBORN, Colorado
MO BROOKS, Alabama
BRADLEY BYRNE, Alabama
ELISE M. STEFANIK, New York

JAMES R. LANGEVIN, Rhode Island
JIM COOPER, Tennessee
JOHN GARAMENDI, California
JOAQUIN CASTRO, Texas
MARC A. VEASEY, Texas
DONALD NORCROSS, New Jersey
BRAD ASHFORD, Nebraska
PETE AGUILAR, California

KEVIN GATES, *Professional Staff Member*
LINDSAY KAVANAUGH, *Professional Staff Member*
NEVE SCHADLER, *Clerk*

CONTENTS

FISCAL YEAR 2017 INFORMATION TECHNOLOGY AND CYBER PROGRAMS: FOUNDATIONS FOR A SECURE WARFIGHTING NETWORK

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES,
Washington, DC, Tuesday, March 22, 2016.

The subcommittee met, pursuant to call, at 3:43 p.m., in room 2118, Rayburn House Office Building, Hon. Joe Wilson (chairman of the subcommittee) presiding.

OPENING STATEMENT OF HON. JOE WILSON, A REPRESENTATIVE FROM SOUTH CAROLINA, CHAIRMAN, SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Mr. WILSON. I call this hearing of the Emerging Threats and Capabilities Subcommittee of the House Armed Services Committee to order. I am pleased to welcome everyone here today for this hearing on the fiscal year 2017 budget request for information technology [IT] and cyber programs.

Lately the Secretary has been highlighting the need for increased innovation in the Department of Defense [DOD] through public-private partnerships—and I was grateful that Secretary Ashton Carter was here yesterday on this issue, so it is right on point—as well as the importance of generating new capabilities to offset growing advantages of future potential adversaries.

I believe that information technology and cyber will both serve as key enablers and, at the same time, present key challenges for the Department as it tries to realize its vision.

In this time of fiscal constraint, I also believe it is equally important to enforce management rigor to make sure that we are squeezing the most out of every defense dollar where it makes sense. We need to learn from industry and use the kinds of business analytics and business intelligence methods that work so well in the commercial sphere. That also means using commercial tools to the maximum extent, especially in areas like business systems and cloud computing.

We need to find better ways to foster and maintain our own human capital to support the acquisition and management of information technology and cyber systems. In looking through this most recent budget request, I want to make sure the Department is emphasizing these two complementary tracks—increased innovation, as well as increased management discipline.

I would like to welcome my distinguished panel of witnesses and appreciate their perspectives on all of these issues. This panel includes the Honorable Terry Halvorsen, Chief Information Officer

[CIO], Department of Defense, the Honorable Peter Levine, the Deputy Chief Management Officer [DCMO], Department of Defense.

I would like now to turn to my friend and ranking member, Mr. Jim Langevin from Rhode Island, for any comments he would like to make.

[The prepared statement of Mr. Wilson can be found in the Appendix on page 25.]

STATEMENT OF JAMES R. LANGEVIN, A REPRESENTATIVE FROM RHODE ISLAND, RANKING MEMBER, SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Mr. LANGEVIN. Thank you, Mr. Chairman. Thank you for convening this hearing. And I want to thank you to our witnesses for testifying today on the President's fiscal year 2017 budget request for information technology and cyber programs.

Last week, we heard about the cyber mission force build and operations from Admiral Rogers, and today we will hear about the infrastructure our warfighters operate within and defend for the enterprise. Cyber Command [CYBERCOM] has advocated for the ability to see the network in order to provide better defense. The joint information environment, or JIE, is the guiding effort for achieving this capability. And today I hope to hear about the progress made under the JIE umbrella, governance for this effort, and service contributions.

Another major undertaking I would like to discuss today is implementing the Department's cloud strategy. The DOD's migration to the cloud has slowed due to laborious certification requirements and an acquisition system unable to keep up with cloud services procurement. This also seems to hinder any efficiency or cost savings that could otherwise be achieved.

Finally, the DOD has been tasked with building and maintaining the IT system for OPM's [Office of Personnel Management's] new National Background Investigation Bureau. While it makes sense the Department provide expertise on building a secure system, I am concerned the DOD is assuming all the risk by providing resources and assuming responsibility for decisions made outside the Department.

As a long-term advocate for cybersecurity within this subcommittee, I am glad we have taken the time to not only discuss the build and operations, but also the infrastructure our cyber warriors operate within every day over the last few weeks.

Again, thank you, Mr. Chairman, and I want to thank our witnesses for being here today to discuss this important topic. And I yield back the balance of my time.

Mr. WILSON. Thank you, Mr. Langevin. And now welcome again to our witnesses. Your written statements will be submitted for the record, so we ask that you summarize your comments in 5 minutes or less, and then after that, each of the persons on the subcommittee will go through a 5-minutes process and Kevin Gates will make sure it is done correctly.

So we now begin with Mr. Halvorsen.

STATEMENT OF HON. TERRY HALVORSEN, CHIEF INFORMATION OFFICER, DEPARTMENT OF DEFENSE

Mr. HALVORSEN. Good afternoon, Mr. Chairman, Ranking Member, and distinguished members of the subcommittee. Thank you for this opportunity to testify before the subcommittee today on the Department's information technology budget request.

As the Department's CIO, I am the principal adviser to the Secretary of Defense for information management, IT, cybersecurity, communications, positioning, navigation, and timing, spectrum management, senior leadership, nuclear command control, and communications matters. Those latter responsibilities are clearly unique to the DOD.

My imperative at the CIO in managing this broad and diverse set of functions is to ensure that the Department has the information and communications technology capabilities needed to support the broad set of Department missions. This includes supporting our deployed forces and cyber mission forces, as well as business and warfighting support functions.

As Secretary Carter has stated, DOD must address strategic challenges across all domains, not just air, land, and sea, but increasingly in cyberspace. The Department's budget includes funding to address these challenges, including IT and cyber investments that are critical to the Department's warfighting, intelligence, and business missions.

As the CIO, I am driving cultural, business, technical improvements, and innovation into DOD's IT and cyber to better support defense missions and operations. My written testimony provides more detailed information on the Department's IT and cyberspace budget and priorities.

I want to emphasize that these efforts require teamwork and partnership within DOD, which includes DISA [Defense Information Systems Agency], USD [Under Secretary of Defense] AT&L [Acquisition, Technology, and Logistics] and Policy, U.S. CYBERCOM, DCMO, and other partners.

External partnerships to DOD will also be critical, to include Congress, industry, and our allies. I strongly believe an expanded partnership with industry will be essential to expanding and maintaining technology advantages, while improving our fiscal accountability.

I thank you for your interest and support, and I look forward to your questions.

[The prepared statement of Mr. Halvorsen can be found in the Appendix on page 26.]

Mr. WILSON. Thank you, Mr. Halvorsen. We now proceed to Mr. Levine.

STATEMENT OF HON. PETER LEVINE, DEPUTY CHIEF MANAGEMENT OFFICER, DEPARTMENT OF DEFENSE

Mr. LEVINE. Thank you, Chairman Wilson, Ranking Member Langevin, and members of the subcommittee.

I am Peter Levine, and I am the Deputy Chief Management Officer of the Department of Defense. Two years ago, this committee enacted legislation which will merge the offices of the DCMO and CIO. However, that legislation does not take effect until the begin-

ning of the next administration, so until that time, the CIO, Mr. Halvorsen, will remain the responsible official within OSD [Office of the Secretary of Defense] for IT, cybersecurity, and many of the other issues addressed in your letter of invitation.

The DCMO's role, until such time as this merger takes place, is limited to reviewing and approving of investments in IT business systems. We do thank you in that regard for last year's NDAA [National Defense Authorization Act], in which you substantially streamlined and gave us more flexibility in the way we do this. We intend to use this flexibility in several ways.

First, we intend to change our focus from the discrete review of each individual small investment and focus more on portfolios, so we can be more forward-looking in our management of business systems. Second, we plan to focus much more on return on investment, so that we can ensure that when we invest in business systems, we actually realize the benefits that we should be able to get out of them, that we actually turn off the legacy systems and reduce manning, where we can develop more efficient and less manpower-intensive processes.

And finally, we are going to work to develop a streamlined process for business systems where we can align our business systems investment process, our CIO process, and our acquisition process into a single process so that we don't have to sequentially go through one after the other and put the program manager through recurring hoops as we go forward.

We are firmly committed to working with you as we try to make the business systems process more efficient and to improve the Department's investment process and look forward to your questions.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Levine can be found in the Appendix on page 35.]

Mr. WILSON. Thank you very much. And we will now proceed with a 5-minute round. I want to commend Lindsay Kavanaugh and Jim Langevin for achieving an extraordinary turnout today. So, congratulations. You did good.

And I will begin with myself. And this is for both of you. What do you see as the major budgetary challenges in this year's President's budget request? Where are we accepting risk based on current budget constraints?

Mr. LEVINE. I will give the gentle answer, which is not enough money. And I will defer to Mr. Halvorsen as to the IT budget specifically.

Mr. HALVORSEN. I certainly echo Peter's first comment about not enough money. I think in the IT area, we are taking some risk in modernization. Some of it will slow. We are trying to balance that and make sure that we don't take that risk in the security side.

The other I think challenge that we are going to have in IT may not be exactly in the budget, and it is going to be the retention of the IT workforce. And frankly, that is going to come down to an economic decision. I happened to be in the valley [Silicon Valley] last week, and, you know, Google announced they are raising the pay for cybersecurity by another 20 percent. That is going to keep impacting our ability to attract talent.

If you ask me about the budget, what keeps me up more at night, that is probably the answer, sir.

Mr. WILSON. And thank you very much. And, Mr. Halvorsen, Chairman Mac Thornberry's most recent defense reform proposal emphasizes prototyping experimentation. Can you tell us what the Department is doing with regard to information technology and cyber programs that highlight these approaches?

Mr. HALVORSEN. Yes, thank you. I think a couple things that we want to think about when we answer this question, much of the innovation today being driven in the cyber and IT business is coming from the commercial sector. We want to be closer tied to the commercial sector, so thanks to some legislation last year, I am able to now put people from DOD inside of business—and we are doing that today—and also have business people on my staff, which we are also doing today.

I think that partnership that we continue to strengthen is a key to us getting the right innovation and getting it on time.

Within the DOD, I want to focus our S&T [science and technology] dollars around the areas the industry isn't going to focus on, and that is going to be on the weapons systems and top-level security systems, where there is not yet much play in the commercial sector, and I think our budget reflects that that is where our emphasis is and also reflects where we are taking risk is around innovation dollars that we would have that were inside the budget for commercial areas that we have taken some risk and are not spending that much.

Mr. WILSON. And, again, I am impressed with the efforts by Secretary Carter to work for public-private cooperation. Additionally, Mr. Halvorsen, in the fiscal year 2017 budget request, the Defense Information Systems Agency, the primary IT provider for the Department, eliminated the S&T funding it had to pursue innovation and technology demonstration. Please explain the rationale for that decision and how this aligns with the Secretary's emphasis on drawing in innovation from the commercial sector.

Mr. HALVORSEN. Yes, we certainly reduced DISA's S&T funding. They still have some R&D [research and development] money. But in the area we reduced it is aligned exactly—I think what we have said before—today, where we are going to get our information, and particularly true for most of DISA's activities, which are supporting our business functions, is from industry and commercial.

So in a constrained budget, in my opinion, that was where we chose to take some risk, because I think I can get that same innovation affect by strengthening our relationships with commercial industry.

Mr. WILSON. Additionally, Mr. Halvorsen, section 901 of the fiscal year 2015 NDAA mandated that the chief information officer begin to exercise authority, direction, and control over the Information Assurances Directorate of the National Security Agency.

Recently, this subcommittee was made aware of a DOD proposal to place that authority, direction, and control back with the Under Secretary for Intelligence. Do you support the Department's proposal? What are the pros and cons of keeping that authority with the chief information officer?

Mr. HALVORSEN. I don't know that the Department has made a formal proposal yet. I know that it is being discussed. Candidly, I would have some concerns about moving it away from the DOD CIO, but more importantly what we are doing is working with the intel side of the Department to form a governance structure that will allow both CIO and intel equities in the IA [information assurances] money to be addressed.

Mr. WILSON. Well, with your background, we would all appreciate any input at any time as we consider these issues.

I now yield to Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman. Again, I want to thank both of our witnesses for being here and what you are doing in the IT and cyber sphere.

So one of the questions I had—and, Terry, you talked about it just a minute ago in terms of, well, the private sector increasing what they are paying their cybersecurity folks, and it is going to be particularly challenging now for us to compete to get that top-end talent.

I know in the NDAA last year, we gave more flexibility to the Department to try to take advantage of that IT talent. You know, for example, allowing potentially—as I envision it—to see private sector to be able to detail for maybe a year or two these high-end individuals that, you know, it would be challenging for us to both afford, attract, and keep for a long period of time.

But, you know, companies have an interest in patriotic duty and want to help secure the Nation in cyberspace. So we made some progress in that with the NDAA, giving some flexibility to the Department. Can you tell me, do you need additional authorities to further take advantage of that talent so that we have the cyber workforce that is as robust as possible and our networks are as secure and as robust as possible?

Mr. HALVORSEN. First, I would thank you for the NDAA last year. That is helping some of the work we are able to do, the excepted workforce in cyber, being able to bring the people in from industry like we are doing now. I do think we will need some legislation that probably changes slightly the rule sets about what we are allowed to do with the industry people.

I think exactly what you stated. We really want to be able to bring them in and have them sit in a position for a year, being able to execute some decisions within the Department, and then go back to industry, just like I think there is a market space today for us to have some of our civilian employees go to industry, and industry would like to have them—and I think we will need to tweak some of the legislation so that could happen more often.

I think we share the vision. In the end, we want more of an in and out, back and forth. And you could really see the career path in cyber IT changing so that it is not an all-civilian or all-government career path, but a much more combined career path. And I think that would serve the Nation well.

Mr. LANGEVIN. Good. I mean, that is exactly where I hope that we are going to be and that is what we want to get to. Please, I hope you will work with us and tell us how we can be of help in terms of additional legislation and language that you need to get to that point.

So as I mentioned in my opening statement, I find it appropriate the Department of Defense is involved in building a new IT system for OPM's new National Background Investigation Bureau [NBIB] that will house sensitive personnel information.

However, I am concerned that the DOD has been given guidance and deadlines that are not realistic and is assuming all responsibility for performance, when the decision-making authority may be shared.

So my questions are, can you describe the Department of Defense's role in building and maintaining a new IT system? Specifically, what is the amount requested for fiscal year 2017, as well as in the out years? Was additional money added to the top line for DISA's role in this effort? Or is it coming out of hide?

What are the resources that are being provided for this effort? Is the current workforce sufficient to meet the demand or will additional personnel be billeted? Will the Department have sole decision-making authority in building and maintaining the system? Or is it shared with OPM and other communities? And what timelines have been established for delivering the system?

And, Mr. Levine, if I could—Levine, I am sorry—what role will you have in doing business process re-engineering to change the way NBIB does business so it fits the IT system, not the other way around? And if you need me to repeat any part of that, I will be glad to. Sorry it is such a long list.

Mr. HALVORSEN. So, sir, what I would like to do, because I do think that question deserves a lot of matter, is I will make some comments on it, but I will also like to take that for the record and get back to you with some of the specific answers.

[The information referred to can be found in the Appendix on page 43.]

Mr. LANGEVIN. Fair enough.

Mr. HALVORSEN. For 2017, it is $95 million. There was a top-line increase to DOD for doing some of this. We will get you the exact numbers across the FYDP [Future Years Defense Program]. And then I would be foolish if I said there is not some concern on DOD's part about how this is going to work, and what I would assure you is from a standpoint of the build, we are going to get the requirements from the group that is looking at how we are going to redo the whole investigation process.

When I have those requirements—and that group starts next week, and we have members on it—we will build a system that supports those requirements that also ensures security. If at any time I think that that is not happening, I will be the first to let you know.

I am comfortable right now that we have worked out a governance process with OPM and OMB [Office of Management and Budget] that makes DOD the decision maker for all of the technical decisions and the security decisions, but I am still concerned and we will have to see how that goes forward. And I will get you more detail on the rest of the question.

Mr. LANGEVIN. I would appreciate it, whatever additional detail you could provide. And I would just assure we stand ready to support you in this effort as you make the transition. And Mr. Levine?

Mr. LEVINE. With regard to the business process re-engineering, we definitely have less of a role in that than we would have if the entire mission had been transferred to the Department of Defense. However, it was never going to be entirely the Department of Defense in any case because as you know the DNI [Director of National Intelligence] establishes security clearance policy, so we are always going to have to work with outside agencies and reconcile differences with outside agencies.

We are undertaking with the Under Secretary of Defense for Intelligence to re-engineer the DOD part of the process. We are looking at continuous evaluation. We are looking at other measures to streamline our organization and streamline our part of the process. And we do still have a piece—significant pieces of the process. It is the investigation piece that OPM has, but not the entirety of the process.

As we do that, we will see places where we are going to want help, we are going to want changes in the OPM piece of the process, and we will have to work that through the interagency, because we don't control it, but we will work it through the interagency process.

Mr. LANGEVIN. Very good. Thank you. I yield back.

Mr. WILSON. Thank you, Mr. Langevin. We now proceed to Congressman Doug Lamborn of Colorado.

Mr. LAMBORN. Thank you. And I will get to the budget implications of this in just a minute, but how active are we in working with allies, NATO [North Atlantic Treaty Organization] allies, Israel, et cetera, in combating cyber threats and cyber attacks?

Mr. HALVORSEN. Extremely active. A couple of the things that we have done that I can talk about in this forum with the Five Eye community,† we actually established last year a CIO Five Eye group that meets physically every 6 months, virtually every quarter. Our next meeting is in London, where cybersecurity is certainly one of the big topics. We have had visits to Israel, exchanging data. That continues.

I just came back from Korea and Japan, where that was a major topic. I can tell you that the NATO partners, Korea, Japan, Germany, have all adopted the DOD cybersecurity scorecard as the basis for measuring how effective we are doing cybersecurity basics across the board, which I think is a big breakthrough.

So we can probably give you some more detail, and we will take that for the record, but they are the major things that we are doing to improve our information-sharing.

[The information referred to can be found in the Appendix on page 44.]

Mr. LAMBORN. Well, that is good to hear. And do you have any recommendations in the budget on maybe making that even stronger? Or, I mean, I know you have a good budget that you are defending right now, but do you see any room for improvement in that area in particular?

Mr. HALVORSEN. You know, I do see room for improvement, but I don't think right now that is a money issue for improvement. I

† "Five Eyes" is an intelligence alliance involving Australia, Canada, New Zealand, the United Kingdom, and the United States.

think it is more of getting all of us aligned to the right principles and basics.

Today we have made good progress within NATO—and as I said, Japan and Korea and Germany—there is some other work we need to do with other partners.

I will be in Estonia in June working some of those issues. And what I would like to do is when I come back from that, I will have a better site picture, is maybe give you some more answers on what I think we might need to do to go beyond some of our traditional allies.

Mr. LAMBORN. Okay. I appreciate that. I would like to follow up on this conversation at another time. Thank you, Mr. Chairman.

I yield back.

Mr. WILSON. Thank you, Mr. Lamborn. We now proceed to Congressman Jim Cooper of Tennessee.

Mr. COOPER. Thank you, Mr. Chairman. First, the Santa Claus question. Both of you mentioned that you would like to have more money. How much? And for what?

Mr. LEVINE. I would say that as the DCMO, my responsibility is finding efficiencies. I am not actually looking for more money. The Department is looking for more money. I am trying to identify efficiencies within the Department where I can free up money so that we can invest more in the long-range science and technology programs and force structure and things that we need to keep our force ready to go today and ready to go in the future. That is where I need more money.

I would defer to Mr. Halvorsen as to specific IT investments.

Mr. HALVORSEN. I think to upgrade some of our legacy systems. And I can get back to you with a number on that. And to tie back with Peter, I think some investment in the legacy systems—and particularly some of the larger both HR [human resources] personnel and pay systems—those investments would do two things for us.

One, we would certainly improve security. There are some issues we need to fix there. Secondly, I think we could improve efficiency, and after we made those investments, I actually think the return on investment would be pretty good. But I will come back to you with a number, sir.

[The information referred to was not available at the time of printing.]

Mr. COOPER. Thank you. Now the Scrooge question. Pentagon is the least auditable of all government agencies. It has been a risk factor for the GAO [Government Accountability Office] for 20 years, the number one risk factor. Will your IT work help the Pentagon get audited faster?

Mr. LEVINE. The answer is yes. Improved business systems, improved financial management systems definitely make an impact. We are much closer today to being auditable than we were 10 years ago. A significant part of that is because of the ERP [Enterprise Resource Planning] investment. But there are many, many hurdles we have to get over that are not IT, and IT can't solve it by itself.

We have policy issues that we have been kicking down the road 10 years that now that we are facing a 2017 deadline, we are finally getting people to be serious about and say, hey, yeah, we ac-

tually have to make those decisions, we have to figure out how we are going to go about that.

So the DCMO co-chairs the governance board, the FIAR [Financial Improvement and Audit Readiness] governance board, which is responsible for trying to drive the Department toward audit with the Comptroller, with Mike McCord. And since I arrived at the Department about 10 months ago, we have been trying—we have set the Department on a program of identifying what our key interim milestones are that we need to hit in order to become auditable.

We have identified a lot of things that should have been addressed 5 years ago or 10 years ago, but we are trying to chip away at them one at a time, and we think that the deadline is extremely constructive in pushing us toward that objective.

The Department seems to have an infinite ability to kick things down the stream and facing a deadline that is 2 years away really helps focus the attention.

Mr. COOPER. Well, some people would say 2017 is next year, not 2 years away.

Mr. LEVINE. It is October 1, 2017. I guess we can—a year and a half is what that is, yes, sir.

Mr. COOPER. Doesn't sound like you are very optimistic about meeting the deadline.

Mr. LEVINE. When I came before the Senate Armed Services Committee for my nomination hearing about almost exactly a year ago, I testified that I had never been confident the Department was going to meet the deadline, and I couldn't change my position just because I was testifying for confirmation.

So I can't change my story now. I am skeptical that we will have done everything we need to do. But I am going to push as hard as I possibly can to get us there.

Mr. COOPER. Okay, now the long-awaited question of the ghost of Christmas past. The Joint Chiefs hack, there was apparently somebody who signed on to an e-mail, like the equivalent from the Nigerian prince or something. Has that person been identified who opened that foolish e-mail? And would it help if they were identified, if they not been identified previously?

Mr. LEVINE. I will say that the people that opened the e-mail have been identified, and we have looked at the reasons why, and in some cases, we did some remediation. In other cases, they had followed the right procedures, up to a point, and we needed to do some more training. That has been put in place to do that, but I would also say that was also one that was caught very quickly.

We had very limited exposure—still would like to do better—but the system and when you look at the volume of e-mail traffic that comes into DOD, how many we get, and the number of people that click, great improvement. We are certainly holding people accountable to a higher standard now.

We have signed out the cyber accountability culture document that was signed by DEPSECDEF [Deputy Secretary of Defense]. Myself, Frank Kendall, and Mike Rogers have signed out the accountability procedures document to make it down to the individual and command level, so I think we have made progress in that area.

I don't think identifying any more individuals at any more level would be helpful right now.

Mr. COOPER. I see my time has expired, Mr. Chairman.

Mr. WILSON. Thank you, Mr. Cooper. We now proceed to Congresswoman Elise Stefanik, of New York.

Ms. STEFANIK. Thank you, Mr. Chairman, and thank you to the panelists for being here today. I have two questions. The first one will be quite broad. The second one will be quite specific. As you are well aware, the threats to the United States have evolved dramatically in the last 10 years. State and non-state adversaries have adapted to a new digital environment quite well. And it is important that the United States invests in the time, training, and infrastructure to counter the whole spectrum of cyber threats.

So as we see in the news, cyber provocation against the DOD infrastructure continues to increase, what is your assessment of the DOD's ability to counter such intrusions today? And what can I tell soldiers that I represent at Fort Drum in my district what we are doing to ensure that they are protected? And what have we learned about the enemy? And how has that changed our approach? That is the first broad question.

Mr. HALVORSEN. Again, I will make some comments on it, but we will take that for the record, because I think it is a good question and we owe you some better details on that.

[The information referred to can be found in the Appendix on page 44.]

Mr. HALVORSEN. We certainly have improved training across the board in the cyber spectrum. The cybersecurity culture issue is one that is on top of the Secretary's desk. We meet every month on the cybersecurity scorecard, and a part of that gets to what is the training of the individuals. The networks themselves are much better today. They are not exactly where we want them. We have got three major efforts to improve that.

The first one is, you are probably aware that the Secretary has directed that this year we move as much of DOD as possible—the ones that are on Windows operating systems—to a Windows 10 baseline. I cannot stress the criticality of us getting that done.

Right now, when you try to look at the visibility of the networks, while we are making improvements, you are doing that across multiple operational systems, multiple baselines. It is impossible to do, do well.

Getting to a single baseline for Windows—and that is about 80 percent to 85 percent of the DOD—will give us the ability to have better visibility. Windows 10 is the first operating system that really thought about security right from the beginning and has in-built features that we will take advantage of.

It will also allow us to go to the next step, which is how do you then start taking and really using cloud computing technology to improve your security? So we are positioned to do that. We have got things we have to get done, and the first one is to get the Windows 10 done.

The other big initiative is to complete the joint regional security stacks. In its simplest forms, what that does is lower our footprint. Today, we have got 1,000 points that you can come in. When the joint regional security stacks are done, we will have less than 100 points. That is a lot easier to defend, and we can focus more on it.

It also stops us from doing our own self-denial attacks, which are also—happen when you are trying to keep aligned over 1,000 different firewalls. We will reduce the firewalls, have better overall security and visibility into the networks. That is what we are doing at the big end.

Ms. STEFANIK. Okay, so the specific questions are actual follow-ups to your answer. When you reference the cybersecurity scorecard process, what is the scorecard exactly? Can you get into more specifics? Can this information and will this information be shared with Congress? Are there plans to expand scorecards beyond cybersecurity? And how does a negative scorecard rating of a DOD component, what is the consequence of that?

Mr. HALVORSEN. Again, we will give you some more details in writing, but here is what I can tell you. The scorecard is looking at what we have defined right now as basic areas that we should be measuring. One of them is, is everybody using a secure token to access DOD systems.

The advantage of that is, is immediate. If you are using the token, A, we know exactly who logged in, when they logged in, where they are at, and it is a lot harder to fake that access. So it is an immediate improvement.

Ms. STEFANIK. Can that information be shared with Congress?

Mr. HALVORSEN. Actually, I am happy to give it to you. We have actually shared it with other committees, and I am happy to send one over when I get back, the current scorecard.

Ms. STEFANIK. And the results of the scorecards that are shared?

Mr. HALVORSEN. The results is right on it. It will show you where we are at. We are not where we want to be in all of the areas. We are measuring ourselves to extremely high standards. One of the things that I just want to say upfront, when you look at cyber, you could hit 80 percent and a lot of people would think that would be good. In cyber, that is not good enough.

So when you see that we are in yellow and, in some cases, red, it is because we are trying to get above in almost every category 95 percent to be green.

Ms. STEFANIK. And the last question is, you talked about the Department's plans to move to the Windows 10 operating system with a mandate to so by a certain date. What is the cost of that transition?

Mr. HALVORSEN. I don't know the exact cost yet. We will get that to you. But what I could tell you, the cost not to do that would be in the billions.

[The information referred to can be found in the Appendix on page 45.]

Ms. STEFANIK. Great, I would look forward to getting more of that in writing afterwards. I yield back.

Mr. WILSON. And thank you, Congresswoman Stefanik. We now proceed to Congressman Pete Aguilar of California.

Mr. AGUILAR. Thank you, Mr. Chairman. Mr. Halvorsen, can you talk to me broadly about in your testimony you talk about cloud computing. Where will cloud computing be in 5 years and in 10 years?

Mr. HALVORSEN. In 5 years, I am hopeful that we will be in an almost complete virtual cloud environment, and cloud defined this

way. We will have private clouds, which are completely private within segments of DOD. We will have private clouds that are just DOD, you know, inside it. And we will have private clouds that are DOD and other parts of the Federal Government. And then we will have hybrid public clouds.

Because of the size of DOD and the Federal Government, we ought to be able to move into where we would have government hybrid clouds hosted in commercial centers as opposed to some of the things I talked about earlier, would be on premise, that would give us the best combination of mission security and value.

Mr. AGUILAR. Is that what you mean when you talk about in page 3 of your testimony mission partner environment, when you are talking about commercially accessible, reconfigurable, and secured data that can be shared with commanders?

Mr. HALVORSEN. A little broader than that. The mission partner environment would certainly use cloud technology, but in that part of the testimony what I am really talking about is how we would be able to support our COCOM [combatant command] commanders as they partner with both traditional and non-traditional allies to support whatever mission it is, to be able to stand up virtual networks on the fly, to be able to do that both at a secure level, at a speed level that we need, and then to keep it fiscally responsible.

Mr. AGUILAR. Can you talk a little bit about how you envision that working and what our stakeholders and coalition partners, what their role in that would be?

Mr. HALVORSEN. So as we can move to cloud technology, one of the things that we have got to recognize, we have got to get—our MPE [mission partner environment] is going to have to be commercial-based. We are not going to be able to do this at, say, a U.S.-only based system. A, other pieces of our allies couldn't afford that, and it is not what they are going to agree to do.

So basing this on a commercial set of technology that also uses commercial classified technology, would allow us to, in the cloud, put together a virtual network that—let's say we had a—this is a really good example, and I think it is in the testimony—and we have done this—let's say we had a natural disaster that had allies now—like the Chinese, the Cubans, us, they are not traditional allies. We could actually stand up a network, once we get some of the technologies in place, that would allow data to be shared.

And let's say we want to share data with China, we want to share data with Cuba, but not exactly the same data. We could do that on a network with the right protections to protect the data that we need using almost commercially available technology today. There is a few pieces that have to be done, but I am—no doubt they will be done by the end of this year.

Mr. AGUILAR. Well, look forward to seeing that development and our discussion about that moving forward. Thank you so much.

I yield back, Mr. Chairman.

Mr. WILSON. Thank you, Congressman Aguilar. We now proceed to Congressman Brad Ashford, all the way from Nebraska.

Mr. ASHFORD. It is a long trip every morning. Thank you, Mr. Chairman, being able to get here.

Congressman Langevin raised the issue that I am trying to understand further. And your answers were good. I want to further

understand it, though, a little bit, because we talk a lot about employee exchanges with the private sector and the need for additional authorities to do that.

It seems to me it is a critical part of the plan going forward and with the talent out there and the demands on the budget and being able to bring people in. And you have, Congressman Langevin, hit it 100 percent, and you did, as well, in your answers.

What do we have to do in order to—I mean, it seems to me that is something we should be able to move on. And what sort of authorities would we need in order to do that?

Mr. HALVORSEN. Again, I would like to come back on record—here is what I would tell you I think the first area. Today there are some statutes that actually prohibit us from giving decision authority to those type of positions. While we certainly want to protect them and make sure that the government is in the end responsible for the decision, if I have got somebody industry—so let's take cloud.

The best cloud engineers today are not in the government. They are not. We have some really good ones, but the best ones today are in industry. We ought to be able to get some of those in. I ought to be able to assign one of them, say, okay, you are the lead cloud engineer for this year that you are doing this work with us, and give them the authority to make decisions, and with some oversight, expend dollars.

Today, under the current authorities, that is hard to do. I need to do some work to figure out what that should look like, and I will come back to you by the summer, if that is good, with some recommendations.

[The information referred to can be found in the Appendix on page 44.]

Mr. ASHFORD. That is really all I have. That is extremely helpful. It seems to me that there are areas where, as you suggest, the private sector or the nongovernmental sector have those expertise. So thank you, Mr. Chairman. That is all I have.

Mr. WILSON. And thank you, Congressman Ashford. And due to how important these issues are, we will proceed with a second round.

And, Mr. Levine, DOD doesn't have a stellar track record in deploying business IT systems. What recommendations would you have to make to improve our abilities to deploy business systems? And, secondly, how can we improve or shape the workforce to better configure, deploy, and manage these business systems?

Mr. LEVINE. First, we don't just not have a stellar record. We have a horrendous record of deploying business systems. I think that of all the things that we do badly, that is one of the ones we do the worst.

So there are a number of things that we need to do on our side of the river to do better. One of the things that we need to do is to recognize the business systems themselves are not going to solve our problems, that what we need to look at is the processes that we are automating, so that if you try to automate an old process without looking at it and figuring out how it works, you are doomed to failure.

We have tried many times to buy an off-the-shelf system and then said to the users of the system—well, have the users of the system come in and tell us, well, that is not exactly the data we want. We want this other data, because that is what we have actually used, and we start tearing apart the guts of an off-the-shelf system. And before you know it, we have spent five times as much to re-engineer the system and to rebuild the system as the cost of the system itself.

We have to control our own appetite, and that is something that we are working on within the Department. In terms of what you could do to help us—so one thing that I would say that you could do to help us, that I hope you will think about, is as we look at the process that we have to go through for business systems, right now, as I said, we are going to try to work with the acquisition community to re-engineer that, because we have a system where we go through an investment review process, we identify a potential solution, and it may be like a $20 million fix to a problem where you do a tinker with an existing system.

We then have to throw it over the threshold, over the transom to the acquisition community that may set up a program office that in itself would cost $20 million, and they will come to us with a solution which is, let's build a whole new system from scratch. Well, that is crazy.

So we are going to try to re-engineer that within the Department. There may be places where we come to you for assistance in doing that re-engineering. And there is one place in particular I would point to, which is right now for what I presume are historic reasons, we have one set of thresholds for what are called major defense acquisition programs [MDAPs].

We have another set of thresholds for what are called major automated information systems [MAIS] programs. MDAPs and MAIS's. The MAIS thresholds are way, way lower, an order of—I don't know, a couple of orders of magnitude lower than the thresholds for MDAPs, but we treat them as the same thing.

What that means is, that when we have an IT—a business system investment, we trigger a process on the acquisition side which is as big and as clumsy as the process we have on the acquisition side when we are buying an aircraft carrier or a fighter aircraft or something like that. And if you are buying a business system, I am not sure that makes sense.

And so I think if you would look at where you treat MAIS systems and MDAPs the same and whether you need to treat them in the same way in legislation, I think that is something constructive that could help us in streamlining our own internal processes.

Mr. WILSON. Well, thank you for being so candid. And additionally, too, hey, technology changes overnight, and so I know it is an extraordinary challenge, but we appreciate both of you on what you are doing. Also, I am grateful—Mr. Halvorsen, I notice your association with Rotary International, your service as a Paul Harris fellow. I am happy to be with you.

So a question, Mr. Halvorsen. Spectrum is a vital resource for the Department. However, it is also one that we are in increasing competition with the commercial sector. What challenges do you see over the next 10 years when it comes to the DOD's use of spec-

trum? What recommendations would you make to improve the responsiveness of the regulatory process to including national security concerns and economic priorities?

Mr. HALVORSEN. So I think today we are in a good spot, hard work with spectrum. We did well with the last auction. And the money is there to change where DOD can move and share spectrum. What I worry about right now is that the private demand for spectrum is going to exceed our ability to keep pace. And we could, if we are not careful, put some national systems at risk.

Some of this takes time. And in this business, I get that time is really valuable and it is money, but there is a physical limitation to how fast we can move the DOD systems either into the ability to share spectrum or out of some spectrum. And I worry—maybe because we are victims of our own success—we have done very well, and the legislation that has been written and the sharing has all worked to date.

But what I hear from industry right now is, well, we want to go faster. And I don't know that we can go much faster today on how we look at spectrum, make the decisions where we can get out, and how we would share.

I would also tell you that while I think industry is starting to look at making their own investments in helping us share, they are just starting that.

And I think one of the things we need to look at is, I am happy to be measured on how DOD is making investments to share—and we ought to think about some measurements that we would give industry to say, how are you doing in making the investments to—your contributions to helping us get to that state?

Mr. WILSON. Well, thank you very much. And now Ranking Member Jim Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman. Again, thanks to our witnesses for being here.

So yesterday I had the opportunity to have a sit-down with Deputy National Security Adviser Avril Haines and the Homeland Security Adviser, Lisa Monaco, to discuss the Comprehensive National Cybersecurity Initiative [CNCI]. And I have certainly been an advocate for many of the proposals under the CNCI for some time, and specifically the appointment of an individual at the executive level to oversee Federal cybersecurity enterprise.

And it is one of the problems that I think previously on the .gov side they really don't have anybody in charge with both policy and budgetary authority that can reach across government and compel departments and agencies to do what they need to do in cyber. Hence, you have things like the OPM breach that happened.

And I think DOD, by the way, is doing a much better job in terms of defending the .mil network. And all of that, as difficult and challenging as it is, it is important. And they are doing good work. But can you describe how DOD fits into the overall CNAP [Cybersecurity National Action Plan], as it is called? And more specifically, how DOD will interact with the new individual, the Federal Chief Information Security Officer who will be appointed to coordinate cybersecurity policies and activities?

Mr. HALVORSEN. Today, and even before the legislation, we partner extensively with the Federal CIO, Tony Scott. I mean, Tony

when he came in brought some new ideas to the Federal side. We are certainly supportive of that, and we will continue to do so.

As the areas that the Federal Government is looking at are applicable to DOD, we will play, and we will play hard, and we will support those. We will continue to advise Tony and the new individual that is appointed on where we think there are things that DOD is doing that should be applied to the rest of the Federal Government, and we will take those things that are really working and apply them within DOD.

I think the establishment of an individual to do that is key to success inside the rest of the Federal Government. And I think there are some opportunities for us to really set that tone.

One of them is, as we rebuild the NBIB and we look at the lessons learned, I know Tony and I have agreed today that we ought to take those lessons learned and apply them across the Federal Government at any place that we see that that is applicable, we will do that.

Mr. LANGEVIN. Okay. What progress has DOD made on cloud computing, specifically integration of capabilities provided by essential service providers, and are there enough certified to create a competitive field? And how are security concerns being addressed?

Mr. HALVORSEN. As for the progress, two things I think I would like to point. We say a lot of times that DOD is behind in cloud. So I wanted to really know if that was true. So I have asked my staff and some outside to take a look at, how does DOD compare in the use of cloud with other Fortune 50 or peer competitors?

We are actually slightly ahead of most of the Fortune 50 in the use of cloud. We are now embarking on doing more, but I don't think DOD is behind. If you look particularly at the financial industry, which has some very strong security similarities to us, they have done exactly what we have done. They take some of their public-facing stuff and they put it into cloud. We have done that with good success.

The next two things that we are doing—and we have now gotten certifications, enough of them, to start being competitive—is to look at how we bring industry into on-premise cloud offerings. We do that right now very limitedly through the NGEN [Next Generation Enterprise Network] contract that the Navy put in place, where actually HP [Hewlett-Packard] is running Navy data centers, to include Navy data centers at the secure level, on-prem [premises], for the Navy.

We are using that model, and we are going to expand that across the rest of DOD.

I will have a couple RFIs [requests for information] out here in the next month. We have a couple contracts that we are going to let that will allow four commercial entities to come in at the Level 4 level in certification, which is right below the classified data. And we have some work being done to allow more companies to partake in the classified space, too. So I actually think we are making good progress. We have got to stay on top of that.

I hope this summer, if the Windows 10 thing goes well, the next announcement that we will make will be that DOD has decided to go to a more complete cloud environment, similar to—and I just

used this as an example—this is not a decision—but similar to what a Windows 365 cloud environment would do. You have to get to that next phase to really take full advantage of the cloud across the board.

Mr. LANGEVIN. Thank you. I just—I know my time is expired, but I will say, I hope along with all of this we are paying maximum attention to the security of the cloud. It does still concern me that, you know, we have the crown jewels in some ways all in one place. And my colleague, Jim Cooper, likes to refer to the cloud as the acronym for Chinese Love Our Uploaded Data. And so security can't be tight enough, as far as I am concerned.

Mr. HALVORSEN. So, Mr. Chairman, can I take one more minute? We agree. And one of the reasons that we are where we are with cloud, it is the same reason the financial industry is where it is with cloud.

We do have some things we have to make sure, and security is right. And one of them is, how do you achieve virtual separation so that you don't get the effect of everything being loaded in one spot and it can be exfiltrated? And if it does get penetrated, how do you quickly shut that off and isolate it? And we are spending a lot of time working with the industry experts in how to do that.

Mr. LANGEVIN. Thank you. Thank you very much.

Mr. WILSON. Thank you, Mr. Langevin, and thank you for your expertise in acronyms. We now proceed to Congresswoman Elise Stefanik, of New York.

Ms. STEFANIK. Thanks, Mr. Chairman. My final question relates to the personnel side of this issue. So one of the challenges that I think we clearly face is ensuring that our cyber, technical, and workforce capabilities can scale economically. And a significant issue for the industry is the clearance process.

Is there any thought being given to an approach for fast-tracking clearance processing for critical skills position, such as computer network operations programmers, to better enable effective support as your mission requirements expand?

Mr. LEVINE. We have a problem with security clearances across the Department of Defense and across the industry. And the problem with prioritizing is how many competing priorities we have. So, yes, that would be a priority, but I can't look across the Department of Defense and say we don't have a dozen other priorities that are at least equal to that. I mean, the number of priorities we have is extraordinary.

The security clearance problem is a problem not only for IT professionals, but also for contractors who are working on weapons systems. It is a problem for the hiring process within the Department of Defense.

That is why we are working to re-engineer our internal processes and why we hope that we will be allowed to help re-engineer some of the OPM processes, as well, as we go forward with this. One of the things that we are very hopeful for is continuous evaluation as a tool that will help speed things up and lower the burdens.

But I have got to say, right now we are runnning continuous evaluation as a pilot program, which means we are running it in addition to all the other requirements. And we are hoping that we

can prove it out so it can be a substitute for some of the requirements that we are going to expedite. We are not there yet.

But it is a hard question, not just for this area, and I don't think the Department can afford to solve it by carving off one universe and treating them better, because the other universes of people we need to get through the security clearance process are also vital to our national security.

Ms. STEFANIK. Mr. Halvorsen, do you have anything to add?

Mr. HALVORSEN. No, I think Peter summed that up very well.

Ms. STEFANIK. Okay, thank you very much. I yield back.

Mr. WILSON. And thank you, Congresswoman Stefanik, for your insight, too. There being no further, we are adjourned.

[Whereupon, at 4:38 p.m., the subcommittee was adjourned.]

A P P E N D I X

MARCH 22, 2016

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

MARCH 22, 2016

Chairman Wilson Opening Statement
Hearing:
"Fiscal Year 2017 Information Technology and Cyber Programs: Foundations for a Secure Warfighting Network"

March 22nd 2016, 3:30pm, 2118

I call this hearing of the Emerging Threats and Capabilities subcommittee of the House Armed Services Committee to order.

I am pleased to welcome everyone here today for this hearing on the Fiscal Year 2017 Budget Request for information technology and cyber programs.

Lately, the Secretary has been highlighting the need for increased innovation in the Department of Defense through public-private partnerships, as well as the importance of generating new capabilities to offset the growing advantages of future potential adversaries. I believe information technology and cyber will both serve as key enablers, and at the same time present key challenges for the Department as it tries to realize its vision.

In this time of fiscal constraint, I also believe it is equally important to enforce management rigor to make sure that we are squeezing the most out of every defense dollar. Where it makes sense, we need to learn from industry and use the kinds of business analytics and business intelligence methods that work so well in the commercial sphere. That also means using commercial tools to the maximum extent, especially in areas like business systems and cloud computing. We need to find better ways to foster and maintain our own human capital to support the acquisition and management of information technology and cyber systems.

In looking through this most recent budget request, I want to make sure that the Department is emphasizing these two complementary tracks: increased innovation, as well as increased management discipline.

I would like to welcome our distinguished panel of witnesses, and appreciate their perspectives on all of these issues. This panel includes:

The Honorable Terry Halvorsen
Chief Information Officer
Department of Defense

The Honorable Peter Levine
Deputy Chief Management Officer
Department of Defense

I'd like to turn now to my friend and Ranking Member, Mr. Jim Langevin from Rhode Island, for any comments he'd like to make.

STATEMENT BY

TERRY HALVORSEN
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

BEFORE THE
HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON
EMERGING THREATS & CAPABILITIES

ON

"Fiscal Year 2017 Information Technology and Cyber Programs: Foundations for a Secure Warfighting Network"

MARCH 22, 2016

NOT FOR PUBLICATION UNTIL
RELEASED BY THE SUBCOMMITTEE
ON EMERGING THREATS &
CAPABILITIES, HOUSE ARMED
SERVICES COMMITTEE

Introduction

Good afternoon Mr. Chairman, Ranking Member, and distinguished Members of the Subcommittee. Thank you for this opportunity to testify before the Subcommittee today on the Department's information technology (IT) budget request. I am Terry Halvorsen, the Department of Defense (DoD) Chief Information Officer (CIO). I am the principal advisor to the Secretary of Defense for information management, IT, cybersecurity, communications, positioning, navigation, and timing (PNT), spectrum management, and senior leadership and nuclear command, control, and communications matters. These latter responsibilities are clearly unique to the DoD, and my imperative as the CIO in managing this broad and diverse set of functions is to ensure that the Department has the information and communications technology capabilities needed to support the broad set of Department missions. This includes supporting our deployed forces, cyber mission forces, as well as those providing mission and business support functions.

Today, I would like to provide you with a brief overview of the Department's IT and cyberspace budget, and highlight the Department's IT priorities. I will also discuss some of the ways in which my office is moving forward in today's dynamic environment, to try and take advantage of technology advances while also recognizing the potential vulnerabilities these technologies may introduce that our adversaries are eager to exploit.

DoD FY17 IT Budget Overview

IT is critical to the Department's warfighting, command, control, and communications systems, computing services, cybersecurity, intelligence and business missions. The DoD fiscal year (FY) 2017 total IT budget request is $38.2 billion, which includes $6.8 billion for the Department's cyberspace operations. The FY2017 cyberspace request represents a $900 million increase from the FY2016 enacted cyberspace budget, and represents increases for our Cyber Mission Forces and other defensive and offensive cyberspace activities. As the Secretary explained, this investment will further our network defenses, build more training ranges for our cyber warriors, and develop cyber tools and infrastructure needed to provide viable cyber options for managing conflict escalation as part of the full range of tools available to the United States.

DoD IT Priorities

The Department's IT priorities, which include modernizing DoD networks, improving information sharing with mission partners, improving DoD cybersecurity, data center consolidation and leveraging cloud technology, and empowering mobile data access, are structured to improve security, efficiency, and effectiveness for DoD IT in the future.

Modernize DoD Networks

The concept of modernizing and integrating the Department's networks and systems to help ensure efficient, effective, secure information sharing with the DoD's internal and external partners is called the Joint Information Environment (JIE). JIE is anticipated to drive a more secure, effective, and efficient IT environment. Its framework comprises a number of discrete,

but related, elements that when integrated should more securely provide the Department with IT capabilities, such as computing and information storage, transfer, and sharing. An important conceptual IT modernization effort, work toward a complete JIE end state will be ongoing.

DoD's top priority to enable the JIE is the Joint Regional Security Stacks (JRSS). Today, DoD has approximately 1,000 disparate security suites facilitated by separate, individualized, localized Service and Agency systems, with more than 5,000 firewalls. Transitioning to the regionally based, centrally managed suite of security appliances, known as JRSS, is anticipated to simplify and secure this environment and significantly reduce the Department's "attack surface" to fewer than fifty points on the network. JRSS provides the baseline for a more coherent, singular security architecture for DoD's cyber defenders. By normalizing security for data and networks across the Services, and consolidating the Department's security posture across its infrastructure, JRSS will increase visibility of the Department's networks and improve cyber situational awareness of those networks, and is essential to the overall cybersecurity of DoD networks, but it also will help DOD reduce costs, improve configuration management, and advance functionality across the network.

Information Sharing with Mission Partners

Coalition communications is an area of critical concern for the Combatant Commanders. The Department regularly works with expected – and sometimes unexpected – mission partners in a range of scenarios. DoD partnered with China and Cuba to provide disaster relief in Haiti, and works with many diverse international partners to help defeat ISIL and train partner nations. The need to securely, reliably, affordably share information with all mission partners has increased exponentially over time, and it likely will only continue on this same course.

To support this need to securely share information with mission partners, DoD is working to implement a commercially based, robust mission partner environment or capability known as the Mission Partner Environment – Information System (MPE-IS). MPE-IS is designed to provide a more cost-effective, rapidly reconfigurable and secure data protection network that enables information sharing to support operations in all environments, giving our Combatant Commanders the flexibility that they need to rapidly add and subtract mission partners as an operation requires. This capability not only allows Commanders to safely, reliably, affordably share the data needed to complete the mission, but to securely separate the information that needs to stay offline, or make it available to a separate set of partners so those partners who need data, have access to it when and where they need it.

Data Center Consolidation and Leveraging Cloud Technology

DoD continues to work to reduce the cost of its IT across the Department through data center consolidation. While I am not yet satisfied with the savings achieved or the current savings projections to-date, the DoD continues to reduce the number of physical sites and administrators needed to operate facilities to not only save money and reduce our footprint, but to also improve security. The Department's data center consolidation efforts support our cybersecurity posture by automating reporting and patch management, and placing vital system assets behind a sustainable layered defense.

While DoD has projected $1.8 billion in cumulative savings through FY2018, the Department is taking steps to aggressively drive more savings. As an example, following a review of Defense Enterprise Computing Centers (DECCs), the Defense Information Systems Agency (DISA) identified two DECCs for closure: DECC Pacific, and DECC Warner Robins. These actions will deliver near term savings without impacting operations. The DECC closures enable DoD to save the resources programmed for facility upgrades, and the migration of capabilities to other sites improves facility utilization overall.

Additionally, the near term establishment of on-premises commercial cloud hosting capabilities for high impact-levels and the increased availability of off-premises commercial cloud capabilities will provide DoD users with the most efficient compute and storage solutions available. Recently the Department established an on-premises commercial cloud capability at the Navy's Allegany Ballistics Lab, and we are engaged in the acquisition of several other on-premises commercial solutions within the Services and DISA. Our objective is to create a competitive environment to increase efficiencies and drive down costs. DoD has also established several options for off-premises cloud services for public facing systems, and we are continuing our efforts with industry to provide commercial cloud services for higher security levels. We are working closely with the Intelligence Community to develop classified cloud capabilities, with both on-premises and off-premises solutions being explored.

Installation-level consolidation of data center facilities supporting local or specialized capabilities will further reduce inventories and enhance savings. DoD is using inventory data to identify instances of multiple data centers within installation boundaries. This information will be used to directly task affected DoD Components to consolidate facilities into a single instance per installation where possible. We have tasked DoD Components to quantify rates for delivering co-location services and Infrastructure as a Service (IaaS) using a common costing tool. The objective is to drive workload to the most efficient providers of these baseline services. Further, using a consistent method to establish these rates enables more direct comparisons to industry providers of like services, thereby enabling the Department to make sound business decisions.

To ensure DoD Components move aggressively, we are taking steps to leverage the authorities provide by the FY2012 National Defense Authorization Act regarding the approval of data center related obligations to drive the Department toward more efficient data center solutions. We are linking the approval of data center obligations to achievement of the requesting Component's Data Center Consolidation and efficiency objectives as documented in their Data Center Consolidation Implementation Plan. DoD Components failing to realize objectives will be denied the ability to obligate funds until corrective actions are taken.

Reducing the data center workload through application rationalization over time (principally within the Business Mission Area (BMA)) will result in additional savings. My office is working with the office of the Deputy Chief Management Officer to review the Department's BMA portfolio beginning with the OSD Components. This review involves a functional review of the systems coupled with total ownership cost estimates to assist in identifying which systems should be retained, re-engineered, or retired. While some application rationalization actions may

be realized in the near term, it is important to realize these efforts are often longer term due to the impact on business processes, data stores, and the need to maintain operations. DoD is committed to making this an ongoing process to ensure DoD drives to and maintains an optimized BMA systems portfolio. Lessons learned from application rationalization within the BMA will be extended to the other defense mission areas as appropriate.

Improving DoD Cybersecurity

Cyber intrusions and attacks by both state and non-state actors have increased dramatically in recent years, putting DoD missions and information at risk. Adversaries continually adapt and evolve in response to cyber countermeasures, threatening DoD networks and systems. DoD is attacked every day in cyberspace, and technology itself allows our adversaries to adapt faster than in any other area of warfare.

Nearly every one of the successful network exploitations that DoD has experienced can be traced to one or more human errors on the network, which makes raising the level of individual awareness and performance in cybersecurity absolutely paramount. DoD is working to transform its cybersecurity culture by improving human performance and accountability through a prioritized a list of key cyber efforts known as the Cybersecurity Discipline Implementation Plan. The plan, which aligns to the Secretary's Cyber Strategy, provides a roadmap to aggressively eliminate preventable cyber vulnerabilities that can put DoD missions at risks. My office tracks overall progress toward the plan through the "DoD Cybersecurity Scorecard," which focuses on four key lines of effort:

1. **Strong Authentication** – to degrade adversaries' ability to maneuver on DoD networks. The Department is mandating the use of approved, more secure two-factor authentication, utilizing DoD Public Key Infrastructure to reduce the ability of adversaries to use stolen credentials to obtain access to DoD networks and systems and degrade adversaries' ability to maneuver in DoD networks. This effort will eliminate the use of weak authentication for users logging-on to DoD networks. Many users still access DoD networks and systems with insecure methods such as usernames and passwords. These methods are very prone to theft from even unsophisticated adversaries.

2. **Device Hardening** – to reduce internal and external attack vectors into DOD information networks. DoD is requiring that all DoD computers be configured to the Department's security standards and that those configurations are kept up to date by patching aggressively. Establish protections such as the inability to click on hyperlinks to reduce spear phishing, which eliminates a significant method that adversaries utilize to successfully attack DoD networks by diminishing use of e-mail as a conduit for access DoD networks.

3. **Reduce the Attack Surface** – to reduce external attack vectors into DOD information networks. The Department is requiring that every Internet-accessible DoD website be protected by DoD Enterprise Security, in a demilitarized zone (DMZ).

4. **Alignment to cybersecurity/computer network defense service providers (CNDSP)** – to improve detection of and response to adversary activity. The Department is requiring that

every DoD mission, computer and network device be properly defended by ensuring that it is monitored by a CNDSP. This ensures that every computer is being tracked for adversary behavior.

Finally, key to the Department's cybersecurity and overall cyberspace operations is our personnel. To address the Department's increased need for skilled cyber personnel as well as the need to increase the cybersecurity skills of IT personnel (e.g., systems administrators) my office is developing a comprehensive strategy to transform multiple segmented, legacy personnel management constructs into a cohesive, mission-focused DoD Cyberspace Workforce Framework. This effort will enhance the Department's ability to recruit, train, develop, and deploy an IT and cyberspace workforce capable of interoperating across organizational structures. To that end, the Department appreciates the authority granted by Congress last year that provides DoD enhanced hiring authority in Cyber and we will continue to work with Congress to identify other authorities that can help DOD recruit and retain personnel in this critical domain.

Empower Mobile Data Access

The Department continues to expand the number of commercial mobile devices that can be used by DoD users. The Department's mobile portfolio includes unclassified and classified mobile capabilities. The basic foundational infrastructure is in place to support the DoD Mobile Unclassified Capability (DMUC), and includes a mobile device manager and a mobile application store and Gateway for unclassified mobility that will leverage commercial carrier infrastructure and provide entry points for classified services. The Department has adopted a multivendor approach, allowing the DoD Components to use the latest commercial devices that offer more capabilities – like mobile apps and GPS – to meet mission needs. These devices, and their applications, are appropriately managed to meet DoD security requirements, but allow the user to have both a personal and work identity that provides flexibility for personal use capabilities, such as personal email or mobile apps for banking, news, and travel information. Moving forward, DoD will evaluate new mobile devices for approval, ensure the mobile infrastructure complies with DoD security policy, and adopt mobility focused business processes to enhance mission effectiveness, promote ubiquitous data access, improve user experience and reduce cost.

A significant challenge in mobility is securing mobile devices, while keeping up with the rapidly changing pace of mobile technologies. As a result, modernizing the DoD security approval process for mobile is one way in which DoD is empowering mobile data access for its users.

Mobile progress on the tactical edge illuminates the untapped potential of mobile capabilities. Tailored applications demonstrate the advantage of adapting mobility to military needs. For example, Air Force flight crews have replaced their heavy paper-based navigational charts and flight manuals with an Electronic Flight Bag (a tablet), which more easily and efficiently allows them to conduct their flight-management tasks. Tactical users have been provided the Android Tactical Assault Kit, a mobile device connected to a tactical network/radio, providing users with up-to-the-second information about the surrounding environment and capabilities such as voice, text chat, video, images, and an interactive, shared, moving map.

New Initiatives

In addition to the above IT priorities, there are several other recently announced initiatives that my office is leading for the Department.

The Deputy Secretary of Defense recently signed a memo directing the Department to complete a rapid deployment and transition to Microsoft Windows 10 Secure Host Baseline. U.S. Cyber Command is the lead for this effort, in consultation with the Chairman of the Joint Chiefs and my office. This mandate – a first in the history of the Department's IT – was based on the need to strengthen our cyber security posture while concurrently streamlining the IT operating environment. DoD desktops, laptops, and tablets using Microsoft Windows will be migrated to a single version of the operating system, improving the Department's cyber posture by establishing a common baseline for our cyber defenders. This migration, which is not without challenges, to a single operating system should also improve the effectiveness and efficiency of how information is shared, while posturing the Department to take full advantage of other technologies and practices that could potentially have a tremendous impact on DoD far beyond the IT/cyberspace environment.

My office is also overseeing the design and implementation of IT to support the recently established National Background Investigations Bureau (NBIB). DISA is responsible for the design and development effort, and $95 million is included in DISA's FY2017 budget request to initiate this effort. The objective is to replace the current background investigations information systems with a new and more reliable, flexible, and secure system in support of the NBIB. DoD will support OPM as they continue to operate the current system. The Department is also conducting a full cybersecurity assessment of the current OPM background investigation infrastructure that will be used to determine the near-term steps that the Department can take to assist OPM with the operation of the current system, as well as near-term steps that OPM itself can take to enhance the security of the current system. It will also inform DoD's design and instantiation of the new investigation system IT infrastructure.

As noted in my introduction, as DoD CIO I am also responsible for PNT, frequency spectrum matters, nuclear command, control and communications, senior leader communications and satellite communications. We are making important progress to enhance DoD's existing positioning, navigation, and timing technologies, including the nationally critical Global Positioning System (GPS). My office is also responsible for overseeing the modernization of the DoD's nuclear command, control and communications capabilities, as well as senior leader communications. DoD, with many Government and industry partners, just completed the most successful spectrum auction ever conducted, raising $43 billion for the U.S. Government, and providing commercial industry access to critical spectrum. My office continues to lead efforts to maximize spectrum access for Government and industry, engaging with industry and partners to develop and exploit technologies that support spectrum sharing and ensure a win-win. In the area of satellite communications (SATCOM), we are driving down costs by better managing requirements at the enterprise level, and by consolidating leases at DISA. Collaboration with the commercial SATCOM industry offer opportunities to identify new business models that will help us further drive down costs, and to take advantage of emerging technologies that will increase capabilities for the Warfighter and for our senior leadership.

In addition, I continue to partner with the Deputy Chief Management Officer to review the DoD's business processes and the supporting IT systems. Our common goal is to increase mission effectiveness, through increased alignment of processes and systems, better understanding of the interrelationships between processes and systems, and to lower the overall costs of doing business through the implementation of cost-driven metrics.

Conclusion

I want to emphasize the importance of our partnerships with Congress, the Federal CIO and Industry. As the importance of cyber and information technology more generally continues to increase these partnerships are essential for our continued success and improvement. The mission and operational impact of our portfolio issues like information sharing, cybersecurity, spectrum management, positioning, navigation, and timing, nuclear command and control and mobility cannot be overstated in today's strategic environment. The role of the CIO in government and industry will continue to evolve and I believe that role will become even more critical as Cyber/IT continues to play an increasingly important role in almost every aspect of our lives.

Thank you for your time and for your continued support of this increasingly critical component of the DoD budget, and I look forward to your questions.

Terry Halvorsen
Chief Information Officer

Terry Halvorsen assumed the duties as the Department of Defense Chief Information Officer effective March 8, 2015. He previously served as the Acting Department of Defense Chief Information Officer. Prior to that, he was the Department of the Navy Chief Information Officer.

As DoD CIO, Mr. Halvorsen is the principal advisor to the Secretary of Defense for Information Management /Information Technology and Information Assurance as well as non-intelligence space systems; critical satellite communications, navigation, and timing programs; spectrum; and telecommunications. He provides strategy, leadership, and guidance to create a unified information management and technology vision for the Department and to ensure the delivery of information technology-based capabilities required to support the broad set of Department missions.

Before serving as the Department of the Navy CIO, Mr. Halvorsen was the deputy commander, Navy Cyber Forces. He began serving in that position in January 2010 as part of the Navy Cyber reorganization. Previous to that, Mr. Halvorsen served as the Deputy Commander, Naval Network Warfare Command. He was responsible for providing leadership for over 16,000 military and civilian personnel and supporting over 300 ships and approximately 800,000 globally dispersed computer network users. In this position he was responsible for the business performance of Navy network operations, space operations, information operations and knowledge management.

Mr. Halvorsen served as an Army intelligence officer in a variety of assignments, including Operations Just Cause and Desert Storm. He holds a bachelor's degree in history from Widener University, and a master's degree in educational technology from the University of West Florida. He is a Rotary International Paul Harris Fellow and an Excellence in Government Leadership Fellow.

Statement of

The Honorable Peter Levine
Deputy Chief Management Officer
Department of Defense

before the

House Armed Services Committee
Subcommittee on
Emerging Threats and Capabilities

On

"Fiscal Year 2017 Information Technology and Cyber Programs: Foundations for a Secure Warfighting Network"

March 22, 2016

Good afternoon Chairman Wilson, Ranking Member Langevin, and Members of the Subcommittee. Thank you for this opportunity to discuss the information technology (IT) budget and the work the Department is doing to improve the effectiveness and security of IT systems in the Department.

My name is Peter Levine, and I have served as the Deputy Chief Management Officer of the Department of Defense since last May. Before that, I spent 28 years working for Senator Carl Levin of Michigan, the last two as Staff Director of the Senate Armed Services Committee.

As the DCMO, I provide direction and advice on improvements to business processes and practices in the Department with a particular emphasis on overhead and mission support functions. Soon after I started last year, the Deputy Secretary asked me to put together a package of efficiencies initiatives that would help free up needed funds to meet emerging needs in the current budget constrained environment. The initiatives that I am currently working on include headquarters reductions, service contract requirements reviews, and business optimization of the commissaries and exchanges. I have also been working on improving business processes, including the hiring process, the conference approval process, and the process for coordinating and issuing DOD directives and other guidance documents.

Two years ago this committee enacted legislation establishing a new Under Secretary for Business Management and Information, which will merge the offices of the DCMO and the CIO. However, the legislation does not take effect until the beginning of the next Administration. Until that time, the CIO – Mr. Halvorson – remains the responsible OSD official for the Joint Information Environment, information assurance activities, and other IT program and budget issues addressed in your letter of invitation.

The DCMO does, however, play a key role in reviewing investments in IT business systems. About two years ago, the Department restructured the Defense Business Council – the body that approves business system investments – so that it is now co-chaired by the Department

DCMO and CIO. The membership of the DBC includes both the DCMOs and CIOs from each of the military departments. This gives us an opportunity to look at investment decisions both in the context of business process improvements and technical compliance with IT standards, to include compliance with cyber security requirements.

Last year's NDAA includes a provision – section 883 – that substantially streamlines legislative requirements addressing the investment review process administered by the DBC. I thank you and your staff for that provision: it will enable us to avoid getting mired in small detail and focus instead on broader issues.

We intend to use the new flexibility in three important ways.

First, we intend to change our focus from the discrete review of each small investment to broader and more comprehensive portfolio reviews. We have designated portfolio managers for key investment areas. These portfolio managers are developing strategic plans, which will be used to guide and evaluate business system investment decisions. This approach has already yielded positive results in the military departments; we hope to achieve similar benefits by applying the same methodology to investments by OSD and the defense agencies and field activities.

Second, we plan to focus more closely on Return on Investment. The Department has long required that a business case analysis be developed for each major business system investment. Unfortunately, we didn't always pay enough attention to what was in these analyses. When we make a major new business system investment, we should have a plan for turning off legacy systems. We should also have a plan for reducing manpower requirements where we can implement more efficient and less manpower-intensive business processes. Some past business case analyses didn't address these issues. Even where they were addressed, we didn't always follow through and ensure that the projected efficiencies and resulting savings were actually achieved. We are working to change that.

Finally, the new statutory flexibility provides an opportunity for the Department to harmonize separate DCMO, CIO, and AT&L approval reviews for business systems investments. The current lack of coordination between these processes often means that business portfolio managers identify a problem, build a business case for the best solution, and then have to hand off to acquisition officials – who start the analysis all over from the beginning. In some cases, I am told that the business case analysis recommends a small tweak to existing systems, but the acquisition system responds by establishing a program office, which may develop an entirely new and expensive solution.

We are currently working with the Under Secretary of Defense for Acquisition, Logistics, and Technology to address this problem by developing a streamlined and coordinated process for business system investments. We believe that our reengineered process should be able to align acquisition oversight, Defense business system certification and CIO technical requirements beginning in the requirements process, carrying through the consideration of alternatives, and supporting the actual acquisition of a final IT capability. Our goal is to better deliver capability, with appropriate oversight, while removing many of the burdens levied on the IT functional and program managers.

Mr. Chairman, the DCMO is firmly committed to closely partnering with the CIO, the USD(AT&L), and other key DOD officials to improve the processes and practices by which the Department acquires and deploys business IT capabilities. By doing so, we hope not only deliver improved mission performance at reduced cost, but also to "bake in" cyber security and information access control from the beginning of the requirements process. I look forward to working with your committee as we continue this effort.

Peter Levine
Deputy Chief Management Officer

Peter Levine has served as the Deputy Chief Management Officer (DCMO) of the Department of Defense since his confirmation by the Senate on May 23, 2015. In this capacity, he is the senior advisor to the Secretary of Defense and the Deputy Secretary of Defense on business transformation and leads the Department's efforts to streamline business processes and achieve greater efficiencies in management, headquarters, and overhead functions.

Prior to his appointment as DCMO, Mr. Levine served on the staff of the Senate Armed Services Committee from August 1996 to February 2015, including two years as Staff Director, eight years as General Counsel, and eight years as minority counsel. Throughout this period, Mr. Levine was responsible for providing legal advice on legislation and nominations, and advised members of the Committee on acquisition policy, civilian personnel policy, and defense management issues affecting the Department of Defense. Mr. Levine played an important role in the enactment of the Military Commissions Act of 2009, the Weapon Systems Acquisition Reform Act of 2009, the Acquisition Improvement and Accountability Act of 2007, the Detainee Treatment Act of 2005, and numerous defense authorization acts.

Mr. Levine served as counsel to Senator Carl Levin of Michigan from 1995 to 1996, and as counsel to the Subcommittee on Oversight of Governmental Management of the Senate Committee on Governmental Affairs from 1987 to 1994. In this capacity, Mr. Levine played a key role in the enactment of the Lobbying Disclosure Act of 1995, the Federal Acquisition Streamlining Act of 1994, and the Whistleblower Protection Act of 1989.

Mr. Levine was an Associate at the law firm Crowell and Moring from 1983 to 1987. He received a Bachelor of Arts degree summa cum laude from Harvard College and a Juris Doctor degree magna cum laude from Harvard Law School

WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING

MARCH 22, 2016

RESPONSE TO QUESTIONS SUBMITTED BY MR. LANGEVIN

Mr. HALVORSEN. The funds for NBIB in DISA's FY17 budget and out year plans were a top line add. The FY17 President's Budget submission requested $20M of O&M and $75M of RDT&E. The initial out year funding profile is presented in the following table:

APPN	Product Title	2018	2019	2020	2021	FY2018 - FY2021
O&M	Background Investigation IT Systems	50,000	150,000	120,000	120,000	440,000
	O&M Total:	**50,000**	**150,000**	**120,000**	**120,000**	**440,000**
RDT&E	Background Investigation IT Systems	50,000	10,000	10,000	10,000	80000
	RDT&E Total:	**50,000**	**10,000**	**10,000**	**10,000**	**80,000**
	GRAND Total	**100,000**	**160,000**	**130,000**	**130,000**	**520,000**

No additional funds from outside of this line are expected to be spent on DOD's effort to support the new IT system. In FY16, OPM will reimburse DOD for initial pre-acquisition prototyping efforts and legacy system support. Funding for these efforts is in the range of $5M.

Forty additional FTEs were added to DISA for the Background Investigations Information Technology (IT) System based on an analogous estimate of the number of FTEs required to architect, design, acquire, implement and sustain a new start IT system. The estimate was generated using a review and analysis of historical programs with the closest scopes and scales of capabilities, adjusted for the high level of concurrency necessary for the rapid delivery of operational capability.

Position/Skillset Required	# of FTE
Program Executive	1
Chief Architect/Engineer	1
Program Manager	1
Deputy Program Manager	1
BPR/Requirements	3
Acquisition Management	4
Systems Engineering	5
Software Design	5
Data Design	5
Information Assurance	5
Testing	3
Implementation and Operations	4
User and Data Transition	2
Total Number of Positions	**40**

The organization structure, specific job descriptions/role, and position grades have not yet been determined and will be confirmed by July as we perform the pre-acquisition planning for the IT system.

The timeline for delivery of the IT system is in the planning phase. A schedule will be developed as part of the pre-Acquisition planning that is currently underway with an expectation to be approved as part of an overall Acquisition Strategy in October 2017.

The DOD CIO is solely responsible for building and maintaining the IT system based on NBIB requirements. The CIO is advised by the Director of OPM and the Federal CIO as part of the NBIB IT Governance Council. [See page 7.]

RESPONSE TO QUESTION SUBMITTED BY MR. ASHFORD

Mr. HALVORSEN. The Department believes the NDAA FY17 House & Senate provisions related to private industry exchanges and ITEP provide the Department the flexibilities needed. We appreciate the support of Congress on this matter. [See page 14.]

RESPONSE TO QUESTION SUBMITTED BY MR. LAMBORN

Mr. HALVORSEN. The DOD CIO International engagement efforts have grown exponentially in the last several years as cyber has emerged as a domain. These objectives align with regional cooperation, information sharing, and interoperability initiatives. Working closely with OUSD(P), the Joint Staff, NSA, DISA, US STRATCOM, US CYBERCOM and Regional Combatant Commands, and the interagency, DOD CIO has established enduring and lasting relationships focused on increased information sharing, promoting foreign disclosure and release, and enhancing communication and collaboration with our allies and partners. DOD CIO led efforts to continue key relationships with the Five Eye (FVEY) partners through the establishment of coordination groups such as the Defense CIO Forum, sharing information and developing mitigations on key cyber issues such as access control, identity management, supply chain security, and secure mobility. Successes in other FVEY fora include information sharing at the classified and unclassified level through the use of U.S. issued FVEY PKI certificates, and exercising incident response information sharing. DOD CIO continues the critical work of fostering objectives of regional cooperation, information sharing, and interoperability across North Atlantic Treaty Organization (NATO), Allies, and Partners. Additional key focus areas include:

- Cybersecurity Posture of NATO: Align security initiatives with NATO mission objectives; ensure that NATO information assets, technologies and data are adequately protected and that NATO's CS workforce is highly skilled and capable.
- Secure Interoperability in Coalition Operations: Ensure the secure interoperability of shared systems between and among the U.S. DOD and coalition partners; identify shared systems and apply the NIST RMF, including developing baselines. Continue development of the Mission Partner Environment (MPE) and continue exercising federated environments with partners.
- Cyberspace Workforce Development: Engage in security cooperation activities that assist coalition partners in developing strategies and policies to build skilled and capable CS workforces. For example recently extended training and exercise participation to partners.
- Cybersecurity Posture of Critical Infrastructure owned by Partner Nations: Engage in activities that assist collation partners in developing strong CS postures of their national critical infrastructure on which DOD missions may depend, including identifying critical systems and applying the security policies.
- Asia Pacific Engagements: Longstanding regular senior allied and partner nation consultations with DOD CIO counterparts in Japan, the Republic of Korea, and Singapore to promote a wide range of information exchange, sharing of best practices, and technical discussions on improving interoperability. [See page 8.]

RESPONSES TO QUESTIONS SUBMITTED BY MS. STEFANIK

Q1. What is your assessment of the DOD's ability to counter cyber threats?

Mr. HALVORSEN. The DOD continues to improve its ability to secure its information systems and networks from adversarial activity. In addition to initiating the Cybersecurity Scorecard, transitioning to Windows 10, and implementing the Joint Regional Security Stacks, the Department is also engaged in protecting our Internet-facing systems, identifying key terrain, and integrating cybersecurity into our evaluation of readiness. In order to ensure the protection of our service members, civilians, contractors, and other DOD personnel, the Department is also engaged in an effort to secure all of its systems that store personally identifiable information. In combination with other ongoing orders and directives, the Department will continue to assess and engage in any areas where we can improve our cybersecurity. [See page 11.]

Q2. What can she tell Fort Drum Soldiers what the Department is doing to ensure that are protected?

Mr. HALVORSEN. As noted above, the Department of Defense is engaged in multiple enterprise-wide efforts to counter cyberspace adversaries. The interconnected nature of DOD systems means that we aim to enhance the cybersecurity of the De-

partment as a whole. We recognize that the security of information systems at one DOD component may rely on the security of information systems at another. Cybersecurity orders, directives, and policies apply across the Department, including the information systems at Fort Drum. The Department will continue to ensure the protection of their information, as well as the information of all our other personnel. [See page 11.]

Q3. What have we learned about the enemy?

Mr. HALVORSEN. The DOD faces a number of cyberspace adversaries ranging from malicious individuals, terrorist organizations, and nation-states with a wide variety of skill levels, capabilities, and resources. These adversaries aim to penetrate our information systems and networks for a number of reasons, including to steal sensitive data or to affect our ability to operate. We have learned that many of these same actors also target a range of other organizations, including the Federal Government, the Defense Industrial Base, and private sector businesses. [See page 11.]

Q4. How has that changed our approach?

Mr. HALVORSEN. The Department actively understands the types of cyber actors that target the DOD. The DOD Cyber Strategy released in April 2015 is driving how the Department is adapting its cyber forces to respond to ever-evolving threats. The strategy guides multiple cybersecurity lines of effort across the Department, including the development of 133 cyber mission force teams by 2018 to strengthen our cyber defense and deterrence postures. The DOD also recognizes the critical need to maintain and improve its proactive, progressive, and coordinated approach for detecting and responding to cyber events and incidents. The DOD's Cyber Incident Handling Program ensures an integrated capability to continually improve the DOD's ability to rapidly identify and respond to cyber incidents that adversely affect the DOD Information Network. It does so in a way that is consistent, repeatable, quality driven, measureable, and understood across DOD organizations. Lastly, to protect the interests of national security, cyber incidents must be coordinated among and across DOD organizations and sources outside the Department, including law enforcement, the intelligence community, and critical infrastructure partners. For example, the DOD interfaces with the Department of Homeland Security on major cyber vulnerabilities via the Cyber Collaboration, Assessment, and Response interagency sessions led by the National Cybersecurity and Communications Integration Center. The Department also works closely with the Defense Industrial Base to enhance their cybersecurity capabilities by sharing unclassified and classified information on cyber threats. [See page 11.]

Mr. HALVORSEN. DOD Components maintain "software assurance" (SA) on licenses for the Microsoft Windows operating system. In addition to the product support and client access licenses that SA provides, SA also includes the right to upgrade to the latest software versions at no additional cost. Therefore, it is expected that DOD Components will be able to upgrade to the Windows 10 operating system with little or no additional expenditures for the operating system software. [See page 12.]

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

MARCH 22, 2016

QUESTIONS SUBMITTED BY MR. WILSON

Mr. WILSON. What is the Defense Department strategy for increasing use of mobility tools, as well as increasing mobile security? What does the DOD intend to do with regard to Bring Your Own Device (BYOD) and BYOD policy?

Mr. HALVORSEN. DOD is already integrating mobility tools in several areas including developing Geospatial Intelligence logistics, and targeting applications. In addition, DOD is establishing Wi-Fi networks to improve coverage and performance. These investments enable improved mobility capabilities for deployment across DOD's enterprise.

DOD is increasing mobile security by migrating to Secure Hash Algorithm 2 (SHA–2), developing a mobile credentialing solution that derives certificates from a DOD user's Common Access Card (CAC), and streamlining the security approval process for devices and software. Following nationally recognized practices enhances security, commercial mobile products must be validated in accordance with National Information Assurance Partnership (NIAP) Protection Profiles (PP) for all parts of the mobile ecosystem (e.g., mobile devices, mobile device management (MDM), mobile apps, wireless infrastructure). Commercial mobile products that process classified information must be approved by the NSA's Commercial Solutions for Classified (CSfC) program.

DOD is continuing to evaluate different private sector proposals to determine if they satisfy Federal security and legal requirements. Initially, a low risk approach of a BYOD implementation would make the most sense for low threat unclassified environments where there would be minimal impact if a data compromise did occur, such as training and student environments. The Department of Navy is currently piloting BYOD. DOD will evaluate lessons learned to determine adoption across the Department.

Mr. WILSON. What activities does the Department have underway to improve the agility of its spectrum-dependent systems? Do you see commensurate activity in the commercial sector?

Mr. HALVORSEN. The complex spectrum environment and evolving threats that warfighters face compel DOD to constantly evaluate a broad array of technology advancements to meet mission requirements. The Department continues to foster efforts, throughout the Military Departments, DARPA, and OSD, that improve agility for DOD's spectrum-dependent systems, which also help military users share better with other spectrum users.

The Department's continued investment in its Electromagnetic Spectrum Strategy is geared toward addressing these needs. The Department's leadership in other efforts such as the National Advanced Spectrum and Communications Test Network, under the auspices of the Commerce Department, its own new Spectrum Access Research and Development Program, as well as the collaborative effort via the National Spectrum Consortium are enabling complementary initiatives to identify and foster development of innovative technologies and techniques for greater agility and flexibility of DOD capabilities, but also improve spectrum sharing and access.

With regard to commensurate activity in the commercial sector, DOD believes that industry is starting to look at making investments to help in their own ability to share with DOD, but they are just at the beginning of that process. As expected of DOD, industry would also need to be held accountable for their own investments in spectrum sharing technologies and how they are contributing toward improved spectrum access. The Department is hopeful that with balanced investment and commitment by agencies and the commercial sector, these efforts will bear lasting results in enabling flexible access to all users in all spectrum bands.

Mr. WILSON. What suggestions do you have to improve coordination and deconfliction for sharing spectrum bands with commercial entities?

Mr. HALVORSEN. It is important to recognize the existing spectrum management and governance mechanisms through the national regulators, i.e., NTIA and the FCC regulatory processes, continue to effectively facilitate shared use of spectrum among Federal users as well as sharing between Federal and non-Federal users (i.e., including commercial entities). Streamlined coordination and deconfliction processes are critical for successful sharing once a national policy decision is made to

implement sharing in a band, noting that sharing requirements differ depending on the band and use scenarios. Technology, sound engineering, balanced policy and regulation, and enforcement are keys tenets that enable successful sharing. Automated coordination and deconfliction capabilities play a critical role, among other necessary tools (e.g., direct human coordination for continued or iterative risk and tradeoff evaluation) for sharing spectrum bands with commercial entities. Continued investment and improvements to automation capabilities would contribute to improved coordination and deconfliction.

Mr. WILSON. You stated in your testimony that DOD shares the same concerns with security in a commercial cloud environment as the financial industry and that the challenge with off-premise commercial cloud is "how do you achieve virtual separation in the cloud so that you don't get the effect of everything loaded in the one spot where it can be removed, and if it does get infiltrated, how do we immediately shut that off and isolate it?" How have you worked with the leading commercial cloud providers to better understand the security mechanisms they use to achieve virtual isolation or physical separation in their commercial offerings?

Mr. HALVORSEN. DOD CIO continues to collaborate with industry through the on-going updates to the DOD Cloud Computing Security Requirements Guide and cybersecurity assessments in support of DOD and FedRAMP provisional authorizations.

Identifying and understanding the threats in a multi-tenant cloud environment remain an on-going challenge. Virtual separations rely on the vendor's software to protect one customer from both malicious attacks and unintentional impacts from other customers. While some vendors have been willing to share information on their mechanism supporting virtual separation, other vendors have been reluctant to share detailed information as it represents the vendor's sensitive intellectual property. Even when the details are shared, fully evaluating these solutions is a significant challenge as each vendor implements their own, proprietary solutions.

In addition to the software itself, weaknesses in the software's configuration and on-going management can also create vulnerabilities. When evaluating multi-tenant cloud services, the Department closely evaluates the vendor's processes for configuration and operations management. All of these factors are taken into account when issuing a provisional authorization at a particular impact-level. Through the Cloud Computing Security Requirements Guide, the Department has implemented a risk management approach that allows Components to match the security and cost of specific cloud services to their specific cybersecurity needs.

Mr. WILSON. We understand that the Marine Corps has implemented a successful "Comply-to-Connect" program that has helped it increase its compliance during network inspection reviews. a. How are those lessons being applied throughout the Department? b. Are requirements for this Marine Corps system reflected in enterprise requirements for network security? c. Are those requirements being integrated into existing programs, like the Host Based Security System, or planned future network defense tools?

Mr. HALVORSEN. Comply-to-Connect (C2C) is a framework addressing several key functions: network access control, deliberate and secure orchestration with other cybersecurity tools (such as vulnerability scanners, software patching tools, and trouble-ticket generation tools) and continuous reporting for the purpose of managing risk. C2C satisfies the asset management/asset detection problem and increases the efficiency by which technical personnel are able to make decisions as to whether an asset has 'complied' with the local enclave/network's security policy to initially connect and remained connect to the network. C2C closes the asset management/asset detection gap in the Department's Information Security Continuous Monitoring (ISCM) Program.

The US Marine Corps has successfully implemented C2C as part of a three-year regional effort covering 3,000 end-points at Camp Lejeune NC. During that period, the effort enabled USMC to meet the objectives of DOD Command Cyber Readiness Inspections (CCRI) with a 90% compliance rate when Marine Corps White Teams conducted a 'no notice' pre-CCRI inspection; and, 93% compliance rate during regularly scheduled inspections executed by DISA. The Marine Corps has successfully enabled the orchestration features of the C2C tools to automate the on-boarding process of new assets "out of the box," to scan and remediate vulnerabilities upon discovery, harden the asset through integration with the Host Based Security System, and register systems into the network security information and event management tool (SIEM). These major muscle movements, in most cases, were executed with minimal touch labor.

The Marine Corps has recently formally validated C2C as a Service-wide requirement and will implement a wider-pilot across Marine Corps assets in the National Capitol Region in FY16. Eventually, the Marine Corps will implement C2C globally

on all Service assets. Comply-to-Connect is endorsed by the Enterprise Cybersecurity Computer Network Defense Senior Steering Group (ESSG). The ESSG is tracking C2C implementation across several Combatant Command, Service and Agency components. The ESSG has directed the development of a Comply-to-Connect concept of operations with a guideline to standardize implementation across component C2C implementations. Department discussions consider C2C as an enhancement to overall cybersecurity across DOD enclaves and networks. The full scope of C2C capabilities have not yet been decomposed into an operational set of requirements. C2C requirements will be considered as part of the Next Generation End Point security strategy and future network defense tools as the Department moves toward assisted automation.

Mr. WILSON. What do you see as the major challenges to improving the management of the Department of Defense? Do you have the business intelligence and business analytics capabilities to provide the same type of support to the Secretary and Deputy Secretary that any CEO in the private sector would have access to?

Mr. LEVINE. The major challenges to improving management of the Department of Defense are threefold. First, the Department is working toward getting the employees at all levels from senior management to worker to understand that there remain ample opportunities for shared, standard processes and procedures that cut across component boundaries. This is particularly true for support activities within the Department. Second, the Department must continue to work with external stakeholders such as veteran support organizations; unions; the White House; and Congress to allow new approaches to these support activities, even if it means changing the structures and processes those stakeholders currently understand and are comfortable with. Finally, in order to provide a basis for both the internal and external engagements, the Department must have a reasonable set of performance measures that show both how the job is being performed today, but also shows at what cost the job is accomplished.

The assessment above leads directly to the answer to the second question. The Department has a robust set of performance information that it can draw upon to make decisions. The DCMO is working with the staff to make this information more readily visible to the senior leadership. For example, the DCMO just provided a detailed progress report on the various efficiency initiatives that Secretary Carter approved in our plans for FY17–20. The DCMO also supported a detailed, performance-based report on how the Department is doing on making progress toward audit readiness. Both these reviews were done with military department Under Secretaries; service vice chiefs of staff; the OSD Under Secretaries; commanders of combatant commands; and the Deputy Secretary of Defense and Vice Chairman, Joint Chiefs of Staff. Comparing to what a CEO in private sector has accesss to, the Department needs to improve these measures by providing a better means to measure how much it costs the Department to achieve the performance outcomes. The Department is working to that end. In fact, achieving an auditable condition will help us move in the direction of measures that show outcomes per dollar spent or per person involved.

Mr. WILSON. What are you doing to improve the quality of data senior leaders have and use for management of the Department?

Mr. LEVINE. The DCMO has been working with the Joint Staff and OSD components to identify performance measures that better describe the major initiatives the Secretary and Deputy Secretary have set for the Department. The DCMO will then use the Deputy's Management Advisory Group (DMAG) to present focused progress reports based on those measures to the military department Under Secretaries and Vice Chiefs; the OSD Under Secretaries; and the Deputy Secretary of Defense and Vice Chairman, Joint Chiefs of Staff. The DCMO and CIO just presented detailed progress status on the various efficiency initiatives approved by Secretary Carter for the FY17–20 period, including measured updates on major headquarters efficiencies; services contracts efficiencies; defense retail; and information technology efficiencies. Working with the OSD Comptroller, we also provided data on Departmental progress toward achieving audit readiness. DCMO is still working with Joint Staff to ensure that progress on readiness is presented and reviewed regularly to the same group.

QUESTIONS SUBMITTED BY MR. LANGEVIN

Mr. LANGEVIN. Mr. Halverson, the Defense Threat Reduction Agency is conducting research & development and prototyping for a Countering Weapons of Mass Destruction (CWMD) Situational Awareness Information System utilizing a cloud-based architecture called Constellation. Constellation is intended to provide an in-

formation sharing platform for the Department of Defense, interagency and international users to be deployed on NIPRNET, SIPRNET, SUN NET and JWICS networks using cross-domain solutions to transfer data across security domains.

What is the role of the Chief Information Officer and Defense Information Systems Agency in Constellation research, development and prototyping? Specifically, what was the role in establishing a security plan to achieve an accredited cross-domain solution, including security milestones and review of proposed security architecture? Has this effort been reviewed in order to determine if architecture elements and applications could be met with existing capabilities, to include computing tools and architectures, or those already being developed? If so, please describe the review and unique capability gaps identified.

Mr. HALVORSEN. The Constellation program is presently in the formative stages of development and prototyping activities needed to identify and mature information technology capabilities to meet CWMD Situational Awareness requirements

DISA and the DTRA Constellation program office are collaborating via the TCRI (Tactical Cloud Reference Implementation) community since the core of Constellation's architecture is DISA's Big Data Platform (BDP), a component of the TCRI.

The Constellation program will eventually require the capability to move data across multiple security domains and DTRA intends to use existing, accredited cross-domain solutions to meet this requirements. DTRA will not develop a new cross-domain solution. The DTRA program office is collaborating with the Defense Intelligence Agency (DIA) Enterprise Cross Domain Services (ECDS) to meet DOD Instruction 8540.01 "Cross Domain (CD) Policy" requirements. Using an ECDS provider allows Constellation to rely upon existing and proven computing tools and architectures, while reducing initial cost and deployment time. The program expects DIA's ECDS to meet Constellation's requirements to pass information between NIPRNet, SIPRNet, and JWICS. Regarding the cross-domain requirement between the public network (SUNet) and our NIPR DOD network, DTRA expects to use Commercial Off the Shelf (COTS) products to perform deep-content filtering and sanitization of public data prior to ingestion into Constellation on the DOD networks.

Mr. LANGEVIN. Can you provide an update on DOD's process for completing the instruction manual for DOD Directive 8140 and when this process might be completed? How is it being accepted by the services?

Mr. HALVORSEN. DOD Directive 8140.01 will be supplemented by an Instruction and at least one Manual. The Instruction will establish policy and procedures and assign responsibilities for the DOD Components to identify, code, track, and report on their respective cyber workforces. A draft of the Instruction completed a first round of informal coordination with DOD Components in December 2015. In the interim, the Department will publish policy guidance to implement the identification and coding requirements of the Cybersecurity Workforce Assessment Act of 2015. The Instruction is scheduled to be completed in 2017 and will incorporate the interim policy guidance.

The Manual(s) will establish procedures, standards, and requirements for qualifications of the DOD cyber workforce, as required by DOD Directive 8140. In 2015, the Department commissioned a study to identify the standards for qualification criteria across cyber work roles. The study, completed in March 2016, provides an analysis of current government, academia, and industry best practices in recruiting, developing, professionalizing, and retaining cyber personnel. In May 2016, the DOD CIO will convene subject matter expert panels to develop specific qualification criteria for each respective information technology and cybersecurity work role. The Manual(s) are scheduled to be completed in 2018.

The Services and Defense Agencies have been involved in the Department's transition to a holistic view of cyber from the onset and continue to play an important role in shaping the policies and DOD Cyber Workforce Framework that will govern and shape the Department's cyber forces into the future.

QUESTIONS SUBMITTED BY MR. KLINE

Mr. KLINE. What is your assessment of the impact of one service acquiring commercial satellite communications on behalf of the Department of Defense as required under section 1610 of the FY16 NDAA?

Mr. HALVORSEN. In the past two years, the Department has realized successes in the commercial satellite communications (COMSATCOM) domain as a result of improved COMSATCOM planning, acquisition and management reforms discussed in the responses to Senate Report 113–44, page 167, accompanying S. 1197 of the NDAA for FY 2014 and Sections 1603 and 1605 of the FY 15 NDAA. Specifically,

the cost of COMSATCOM services has been declining, DISA's operational responsiveness has improved, and DISA's SATCOM pathfinders are yielding efficiencies in the use of the acquired services. Likewise, the Air Force pathfinders are providing valuable lessons related to investments in COMSATCOM solutions that will further drive acquisition and utilization efficiencies as part of our Wideband SATCOM Plan. To the extent they can, these lessons learned will be folded into the Wideband SATCOM Analysis of Alternatives directed by Section 1611 of the FY 16 NDAA.

With that in mind, the Department is concerned that restructuring this approach by assigning a single agent for acquisition of COMSATCOM services and investment in COMSATCOM capability may ultimately result in increased cost and decreased operational responsiveness for DOD customers with no noticeable improvement in DOD's overall SATCOM "planning, acquisition, and management" processes and governance. To that end and in response to Section 1610 of the FY 16 NDAA, my office has tasked the Air Force to evaluate, and provide the cost estimates to implement, alternative courses of action to satisfy the intent of Section 1610. These plans and cost estimates will be evaluated and coordinated with the Services and Combatant Commands with their inputs incorporated in the DOD response to Section 1610.

Mr. KLINE. Section 1610 of the FY16 NDAA requires the Department of Defense to designate a single acquisition agent to acquire commercial satellite communications. Have the major users (services and combatant commanders) of commercial satellite communications provided input to the Chief Information Officer regarding changes to commercial satellite acquisition and management required in the FY16 NDAA?

Mr. HALVORSEN. In response to Section 1610 of the FY 16 NDAA, DOD CIO has tasked Air Force to evaluate, and provide the cost estimates to implement, alternative courses of action to satisfy the intent of Section 1610. These plans and cost estimates will be evaluated and coordinated with the Services and COCOMs with their inputs incorporated in the DOD response to Section 1610.

QUESTIONS SUBMITTED BY MR. LAMBORN

Mr. LAMBORN. What is the status of the DOD Commercial Partnership Data Distribution Center you mentioned in last year's testimony, and when will you have a secure commercial cloud capability operating from within a DOD data center facility?

Mr. HALVORSEN. IBM's Cloud Managed Services for Government (IBM–CMSG) is an Infrastructure as a Service cloud provided from the Navy's Allegany Ballistics Laboratory (ABL) in West Virginia. It was granted a DOD provisional authorization at level 5 (Unclassified-FOUO) for use by the Defense Logistics Agency and Naval Sea Systems Command in February 2016.

Two additional acquisitions of a secure, on-premise clouds are currently underway in the Army and the Defense Information Systems Agency:

The Army's effort will assess the feasibility and value of an on-premises, commercially owned/commercially operated cloud service offering at Redstone Army Arsenal. The Army is taking a "statement of objectives" approach to obtaining this capability in order to fully partner with industry, learn from its experts and implement commercial best practices for cloud migration and security. The intent of the pilot is to produce a secure, commercial cloud capability by fiscal year 2017 that meets all requirements for hosting sensitive National Security Systems at information security impact levels 5 (FOUO) and 6 (Secret). The Army released a request for information in November 2015 and held an industry day on 21 January 2016 with interested parties.

DISA is also exploring the use of commercial infrastructure services residing in DOD facilities to implement an "on-premises private" infrastructure service for the DOD community and mission partners. The initial phase of this effort is referred to as milCloud 2.0 Phase 1 (M2P1). DISA released an RFI (PL83220028) on February 12, 2016, to assess the marketplace's interest in providing on-premises infrastructure services from within DOD data center facilities and to get advice on refining the businesses model process. DISA is currently reviewing RFI responses and refining their approach for a planned award in first quarter FY17.

Mr. LAMBORN. The DOD has access to a vast amount of data generated by its own IT devices, networks, and equipment. How is the Department leveraging this data to reduce costs, improve operations, and strengthen cybersecurity?

Mr. HALVORSEN. DOD leverages data from a wide array of DOD IT devices, networks, and equipment to guide it in reducing costs, improving operations and strengthening cybersecurity (CS) across the department in support of warfighting and business mission areas. DOD is committed to constant improvement in its data

collection and analytic efforts to ensure the best possible mission outcomes for our warfighters and the most efficient use of taxpayer dollars.

DOD CIO led the development of the SECDEF Cybersecurity Scorecard populated with internal DOD data against 11 key cyber measures. The measures were informed by our understanding of how we are vulnerable to adversary attacks as described in the 2015 DOD Cybersecurity Discipline Implementation Plan. This management tool therefore allows the Secretary to assess progress against goals which will tangibly reduce vulnerability. Further, it focuses each of the Department's 46 component organizations and the Department as a whole on assessing and addressing vulnerabilities. Most of the Scorecard data is pulled from automated cybersecurity tools currently deployed across the Department and we are actively working to build on this momentum to improve how data is automatically collected, integrated, analyzed and reported across the Department.

The SECDEF Cybersecurity Scorecard is one very visible element of the Department's overall effort to use data to reduce costs, improve operations, and strengthen cybersecurity. The Defense Information Systems Agency (DISA), working with the Military Departments and USCYBERCOM, is leading the effort to build a joint interoperable (common) platform to collect and visualize vast amounts of data. This capability is called the Big Data Platform (BDP).

The BDP's value is three-fold:

First, it is a computing information system infrastructure (software) that can be easily shared. Sharing this infrastructure enables the ability to create common visualization analytics that can then be distributed across operational centers, ultimately reducing work efforts, re-work and overall costs. Moreover, it leads to a common way of operating, strengthening Tactics, Techniques and Procedures (TTPs) to aid in the cybersecurity mission.

Second, the BDP is data agnostic. The platform can collect vast amounts of data in any mission area (cyber, business, personnel, etc.). The concept is that the data can be collected and queried (correlating analytics) to answer an infinite amount of operational questions (use cases/scenarios). Data drives situational awareness and an operational use case drives what data should be collected and visualized. The BDP inherently drives the DOD toward the development and implementation of data standards. An example would be the Structured Threat Information eXpression and Trusted Automated eXchange of Indicator Information (STIX)/TAXII) efforts.

Third, the BDP is a critical part of an information ecosystem that includes cybersecurity sensors, information sharing systems and security and incident management (SIEM) capabilities. As the DOD collectively consolidates security architectures and TTP's, the BDP is being architected to support this consolidation. An example is the design and implementation of the Joint Regional Security Stack (JRSS) within Joint Information Environment (JIE) Framework.

Mr. LAMBORN. Recently, the Secretary of the Air Force stated that over time, the AF wants to transition more and more of network operations and maintenance to the private sector. You also spoke of leveraging the private sector as well, specifically as it relates the use of cloud computing capabilities. Currently these potentially outsourced functions are performed by military personnel as well as DOD civilians. What happens to the thousands of civilians when this occurs? Will they all get re-rolled to defensive operations? Do current legal authorities permit the use of title 5 civilian personnel in title 10 defensive cyber activities? If not, what authorities would the Congress need to change or add within the U.S. Code?

Mr. HALVORSEN. The Air Force, like all DOD Components, is responsible for deploying capabilities and aligning their workforce to meet mission needs. Any military personnel or DOD Civilian efficiencies realized as a result of transitioning network operations and maintenance functions to the private sector will be available for the Services and Agencies to repurpose. At the Department-level, DOD Directive 8140.01 unites the management of all cyber skill areas under a single governance construct. This construct is bolstered through the use of the DOD Cyber Workforce Framework, which will be used to develop qualification criteria for all cyber work roles. These qualification criteria will provide the Components with the training requirements for military and civilian personnel who will remain in cyber work roles. DOD civilians currently serve across the Cyber Mission Forces (CMF) and can, consistent with law and policy, participate in the CMF's Title 10 activities.

○